Lineare Algebra I
für die Fachrichtung Informatik
Wintersemester 2023/24

Karlsruher Institut für Technologie

Lineare Algebra I
für die Fachrichtung Informatik
Wintersemester 2023/24

Algebren

&

Polynome

Halbgruppe

$(S, *)$

S Menge

$*: S \times S \to S$

...

Monoid

$(S, *)$

S Menge

$*: S \times S \to S$

...

Gruppe

$(G, *)$

Menge

$*: G \times G \to S$

...

$\mathbb{K}$ Körper

Ring

$(R, +, \bullet)$

R Menge

$+: R \times R \to R$

$\bullet: R \times R \to R$

...

$\mathbb{K}$-Vektorraum

$(V, +, \cdot)$

V Menge

$+: V \times V \to V$

$\cdot: \mathbb{K} \times V \to V$

...

$\mathbb{K}$-Algebra

$(A, +, \bullet, \cdot)$

A Menge

$+: A \times A \to A$

$\bullet: A \times A \to A$

$\cdot: \mathbb{K} \times A \to A$

...

Def: 5.4.2

$\mathbb{K}$ Körper

Eine $\mathbb{K}$-Algebra (oder Algebra über $\mathbb{K}$)

A Menge

$+ : A \times A \to A$

$\bullet : A \times A \to A$

$\cdot : \mathbb{K} \times A \to A$

ist ein Tupel $(A, +, \bullet, \cdot)$,

sodass

- $(A, +, \bullet)$ ein Ring ist.
- $(A, +, \cdot)$ ein $\mathbb{K}$-Vektorraum ist
- $\forall a, b \in A$ $\forall \lambda \in \mathbb{K}$: $(\lambda \cdot a) \bullet b = a \bullet (\lambda \cdot b) = \lambda \cdot (a \bullet b)$.

$(A,+,\bullet,\cdot)$ kommutativ $:\Longleftrightarrow$ $(A,+,\bullet)$ kommutativ

$\Longleftrightarrow$ $(A,\bullet)$ kommutativ

$a \in A$ invertierbar in $(A,+,\bullet,\cdot)$ $\Longleftrightarrow$ a invertierbar in $(A,+,\bullet)$

$\Longleftrightarrow$ a invertierbar in $(A,\bullet)$

$\dim_{\mathbb{K}}(A,+,\bullet,\cdot)=n$ $:\Longleftrightarrow$ $\dim_{\mathbb{K}}(A,+,\cdot)=n$

$B \subseteq A$ $\mathbb{K}$-Unteralgebra $:\Longleftrightarrow$ $B \subseteq A$ $\mathbb{K}$-Untervektorraum und $B \subseteq A$ Unterring

$\varphi: A \longrightarrow B$ $\mathbb{K}$-Algebra-Homomorphismus $:\Longleftrightarrow$ $\varphi: A \longrightarrow B$ $\mathbb{K}$-linear und $\varphi: A \longrightarrow B$ Ring-Homomorphismus

$\mathbb{K}$-Algebra-Endo/-Iso/-Automorphismus analog.

Bsp:

$\mathbb{K}$ Körper

$$A \times A \to A$$
$$\mathbb{K} \times A \to A$$

$(\mathbb{K}, +, \cdot, \cdot)$

$(\mathbb{K}^{n \times n}, +, \cdot, \cdot)$, $n \in \mathbb{N}$

Matrixprodukt

skalare Mult.

$(\mathrm{End}_{\mathbb{K}}(V), +, \circ, \cdot)$

V $\mathbb{K}$-VR

Verkettung

$\dim V = n$

B geordn. Basis

$$\mathrm{End}_{\mathbb{K}}(V) \cong \mathbb{K}^{n \times n} \quad \text{als } \mathbb{K}\text{-Algebren.}$$
$$\varphi \longmapsto M_{BB}(\varphi)$$

$(\mathbb{K}^J, +, \cdot, \cdot)$

J Menge

punktw. Mult.

punkt. Skalieren

$\mathbb{L}$ Körpererw. von $\mathbb{K}$

$$\mathbb{R} \subseteq \mathbb{C} \qquad \mathbb{Q} \subseteq \mathbb{C}$$
$$\mathbb{Q} \subseteq \mathbb{R} \qquad \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2 \subseteq \mathbb{F}_4$$

Bsp.:

$\mathbb{K}$ Körper

	Dimension	Kommutativ?	Einheitengruppe (invertierbare Elemente)
$\mathbb{K}$	1	Ja	$\mathbb{K}^\times = \mathbb{K}\setminus\{0\}$
$\mathbb{K}^{n \times n}$ $n \in \mathbb{N}$	n^2	nein, $n \geq 2$	$GL(n, \mathbb{K})$
$End(V)$ V $\mathbb{K}$-VR	n^2 wenn $\dim V = n$ ∞ wenn $\dim V = \infty$	nein, wenn $\dim V \geq 2$	$Aut(V)$
$\mathbb{K}^J$ J Menge	$\|J\| \in \mathbb{N}_0 \cup \{\infty\}$	Ja	$(\mathbb{K}\setminus\{0\})^J$
$\mathbb{L}$ Körpererw. von $\mathbb{K}$	Kommt drauf an.	Ja	$\mathbb{L}\setminus\{0\}$
$\mathbb{K}[X]$	∞	Ja	$\mathbb{K}^\times = \mathbb{K}\setminus\{0\}$

$\mathbb{K}$ Körper

$\mathbb{K}[X] :=$ die Menge aller Polynome in X mit Koeffizienten aus $\mathbb{K}$

$3X^3 - 5X$

$X^2 + 1$

$$(3X^3 - 5X)(X^2+1) = 3X^5 + 3X^3 - 5X^3 - 5X$$
$$= 3X^5 - 2X^3 - 5X$$

$$7(X^2+1) = 7X^2 + 7$$

$$p = 3X^3 - 5X \in \mathbb{Q}[X]$$

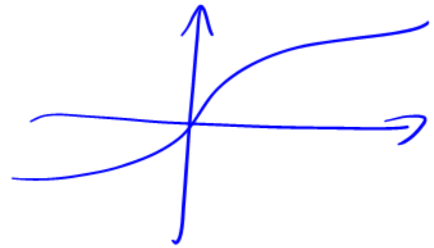
$$3(\sqrt{2})^3 - 5X = \dots$$

$$3\pi^3 - 5\pi =$$

$$3i^3 - 5i = -8i$$

z.B.:

$$\arctan: \mathbb{R} \to \mathbb{R}$$



$\cancel{\arctan(i)}$

$$M = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \in \mathbb{Q}^{3\times 3}.$$

$$p(M) = 3M^3 - 5M$$

$$= 3\begin{pmatrix} 8 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} - 5\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 14 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 4 & -2 \end{pmatrix}$$

$$\varphi \in \mathrm{End}(V)$$

$$p(\varphi) = 3\varphi^3 - 5\varphi$$

$$= 3\,\varphi \circ \varphi \circ \varphi - 5\varphi$$

$$\in \mathrm{End}(V).$$

$$p = a_0 X^0 + a_1 X^1 + a_2 X^2 + a_3 X^3 + a_4 X^4 + \dots + a_n X^n$$

$$p \in LH(X^0, X^1, X^2, \dots)$$

$$K[X]$$

Diese Darstellung ist eindeutig.

Def 5.4.6 $\mathbb{K}$ Körper

(a) A $\mathbb{K}$-Algebra, $X \in A$

$X^0, X^1, X^2, X^3, \ldots$ paarw. verschieden

und $\{X^k \mid k \in \mathbb{N}_0\}$ ist eine Basis von A

Dann heißt A Polynomalgebra in der Variablen X über dem Körper $\mathbb{K}$.

Wir schreiben dann $\mathbb{K}[X] = A$.

(b) $p \in \mathbb{K}[X]$ heißt (formales) Polynom

$$p = \sum_{k=0}^{n} a_k X^k \qquad \text{mit } a_k \in \mathbb{K}$$

Koeffizienten von p

(c) $\forall p \in \mathbb{K}[X] \setminus \{0\}$, definiere den Grad von p als

$$\deg(p) := \max\{k \in \mathbb{N}_0 \mid a_k \neq 0\} \in \mathbb{N}_0$$

$$\deg(0) := -\infty$$

Jedes $c \in \mathbb{K}$ identifizieren wir mit $c \cdot X^0 \in \mathbb{K}[X]$.

Also $\mathbb{K} \subseteq \mathbb{K}[X]$.

$K = \mathbb{Q}$

$q = X^2 + 1$

$M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \in \mathbb{Q}^{2\times 2}$

$q(M) = M^2 + \mathbb{1}$

$= \begin{pmatrix} 4 & 0 \\ 0 & 9 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 10 \end{pmatrix}.$

$\varphi \in End(V)$

$X^2 + 1$

$q(\varphi) = \varphi \circ \varphi + id_V$

$a^2 + 1_A$

Satz 5.4.11: $\mathbb{K}$ Körper

A Algebra über $\mathbb{K}$ (z.B. $A = \mathbb{K}$, $A = \mathbb{C}$, $A = \mathbb{K}^{n \times n}$)

$a \in A$

Dann gibt es einen eindeutigen $\mathbb{K}$-Algebra-Homomorphismus

$$\mathbb{K}[X] \longrightarrow A, \quad p \longmapsto p(a)$$

der X auf a abbildet,

genannt **Auswertungshomomorphismus**. (Einsetzungshomomorphismus)

Bw: Konstruiere $\varphi: \mathbb{K}[X] \longrightarrow A$

φ $\mathbb{K}$-linear

φ multiplikativ

$$\left(\begin{array}{l} \varphi(1) = 1_A \\ \varphi(X) = a \\ \varphi(X^2) = a^2 \\ \varphi(X^3) = a^3 \end{array}\right)$$

$$\varphi(X^n) = a^n \quad \forall n \in \mathbb{N}_0$$

Per Def. ist $\{X^n \mid n \in \mathbb{N}_0\}$ eine Basis von $\mathbb{K}[X]$.

Also Satz 4.2.14 sagt: $\exists\ \varphi: \mathbb{K}[X] \longrightarrow A$ $\mathbb{K}$-linear

$\varphi(X^k) = a^k$. φ eindeutig.

z.z. φ multiplikativ, d.h. $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$.

$$p = \sum_{k=0}^{m} c_k X^k \qquad q = \sum_{l=0}^{n} d_l X^l$$

$$pq = \left(\sum_{k=0}^{m} c_k X^k\right)\left(\sum_{l=0}^{n} d_l X^l\right)$$

$$= \sum_{k=0}^{m} \sum_{l=0}^{n} c_k d_l X^{k+l}$$

$$\varphi(pq) = \sum_{k=0}^{m} \sum_{l=0}^{n} c_k d_l \varphi\left(X^{k+l}\right)$$

$$= \sum_{k=0}^{m} \sum_{l=0}^{n} c_k d_l \quad a^{k+l}$$

$$= \left(\sum_{k=0}^{m} c_k \, a^k \right) \left(\sum_{l=0}^{n} d_l \, a^l \right) = \varphi(p) \cdot \varphi(q).$$

Satz 5.4.8

$\mathbb{K}$ Körper

(a) Es gibt eine Polynom-Algebra

$\mathbb{K}[X]$,

(b) Diese Algebra ist eindeutig bis auf eindeutigen Isomorphismus, d.h.

Wenn $A = \mathbb{K}[X]$ und $B = \mathbb{K}[Y]$

Dann gibt es genau einen $\mathbb{K}$-Algebra-Isomorphismus

$$\varphi : \mathbb{K}[X] \longrightarrow \mathbb{K}[Y]$$

mit $\varphi(X) = Y$.

Bw-Versuch: $\mathbb{K} = \mathbb{R}$.

$$\mathcal{P} = \{ f : \mathbb{R} \to \mathbb{R} \mid f(t) = a_0 + a_1 t + \dots + a_n t^n, \ a_i \in \mathbb{R} \}$$

Polynomfunktion.

$$\subseteq \left(\mathbb{R}^{\mathbb{R}}, +, \cdot, \cdot \right) \quad \mathbb{R}\text{-Algebra.}$$

Unklar: Sind $(1, t, t^2, \dots)$ lin. unabh?

$$(\forall t \in \mathbb{R}) \ \sum_{k=0}^{n} a_k t^k = 0 \ \overset{??}{\Longrightarrow} \ (\forall k \ a_k = 0)$$

Das ist richtig. :)

Für $\mathbb{K} = \mathbb{F}_2$ klappt das NICHT.

$$\left|\mathbb{F}_2^{\mathbb{F}_2}\right| = 2^2 = 4.$$

$$\left|\mathbb{F}_2[X]\right| = \infty.$$

$$p = X^2 + X \in \mathbb{F}_2[X]$$

$$p(0) = 0^2 + 0 = 0$$

$$p(1) = 1^2 + 1 = 0.$$

Die Polynomfunktion $\mathbb{F}_2 \longrightarrow \mathbb{F}_2$, die zu $X^2 + X$ gehört, ist die Nullfunktion.

Bsp:

$$V = \mathbb{K}^{(\mathbb{N}_0)} = \{ (x_k)_{k\in\mathbb{N}_0} \mid \exists n \in \mathbb{N} \ \forall k > n \ x_k = 0 \}$$

$$= LH \left(\{ e_j \mid j \in \mathbb{N}_0 \} \right)$$

$$e_j = (0, 0, \ldots, 0, \underset{\substack{\uparrow \\ j}}{1}, 0, \ldots)$$

$\{ e_j \mid j \in \mathbb{N}_0 \}$ Basis für V.

Def. $* : V \times V \longrightarrow V$, sodass $(V, +, *, \cdot)$ $\mathbb{K}$-Algebra wird.

$X = e_1$ und $e_j = X^j$.

$$\left(\sum_{j=0}^{n} \alpha_j e_j \right) * \left(\sum_{k=0}^{m} \alpha_k e_k \right)$$

$$\sum_{j=0}^{n} \sum_{k=0}^{m} \alpha_j \alpha_m e_{j+k}$$

$$\sum_{N=0}^{n+m} c_N e_N$$

$$\text{mit } c_N = \sum_{j+m=N} \alpha_j \alpha_m$$

$*$ nennt man auch Faltung (Convolution).

. . .

b) $\mathbb{K}[X]$ $\mathbb{K}[Y]$

5.4.11 $\exists\, \varphi: \mathbb{K}[X] \longrightarrow \mathbb{K}[Y]$ eindeutig $\mathbb{K}$-alg-Homom

mit $\varphi(X) = Y$

5.4.11 $\exists\, \psi: \mathbb{K}[Y] \longrightarrow \mathbb{K}[X]$

mit $\psi(Y) = X$.

$$\varphi \circ \psi = id_{\mathbb{K}[Y]}$$

$$\psi \circ \varphi = id_{\mathbb{K}[X]}.$$

Lemma 5.4.10

$\mathbb{K}$ Körper

$p, q \in \mathbb{K}[X]$

(a) $\deg(p+q) \leq \max\left(\deg(p), \deg(q)\right)$

(b) $\deg(pq) = \deg(p) + \deg(q)$

(damit diese Formeln auch für 0 gelten, muss $\deg(0) = -\infty$

$(-\infty) + k = -\infty$.)

Bw: einfache Rechnung (siehe Skript)

Lemma 5.4.13

$\mathbb{K}$ Körper

$p \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$

Dann sind äquivalent:

$\boxed{p(\lambda) = 0} \iff \boxed{\exists q \in \mathbb{K}[X] : p = (X - \lambda) \cdot q}$

Bw: „$\Leftarrow$": $p = (X - \lambda) \cdot q$

$$p(\lambda) = \underbrace{(\lambda - \lambda)}_{=0} q(\lambda) = 0.$$

$0^0 = 1$

$0^1 = 0$

$0^2 = 0$

$0^3 = 0$

„$\Rightarrow$": $\boxed{\text{Falls } \lambda = 0:}$ $p = \sum_{j=0}^{n} c_j X^j$ $\quad 0 = p(0) = \sum_{j=0}^{n} c_j 0^j = c_0$

$$p = \sum_{j=1}^{n} c_j X^j = X(c_1 + c_2 X + c_3 X^2 + \ldots)$$

$$= (X-0)\underbrace{\left(c_1 + c_2 X + \dots\right)}_{q}$$

$\boxed{\text{Falls } \lambda \text{ allgemein:}}$

$$Y = X - \lambda \in K[X]$$

$$X = Y + \lambda$$

$$p = \sum_{j=0}^{n} c_j (Y+\lambda)^j = \sum_{j=0}^{n} d_j Y^j$$

$$0 = p(\lambda) = \sum_{j=0}^{n} d_j 0^j = d_0$$

$$p = \sum_{j=1}^{n} d_j Y^j = Y\left(c_1 + c_2 Y + \dots\right)$$

$$= (X-\lambda)\left(c_1 + c_2 (X-\lambda) + \dots\right).$$

Satz 5.4.15

$\mathbb{K}$ Körper

$p \in \mathbb{K}[X] \setminus \{0\}$.

$n = \deg(p)$.

Dann hat p höchstens n Nullstellen in $\mathbb{K}$.

Bw: Wenn p keine Nullstellen hat: ✓

Wenn $p(\lambda) = 0$

$$p = (X - \lambda)\, q$$

$$\deg(p) = \underbrace{\deg(X-\lambda)}_{1} + \deg(q) \implies \deg(q) = \deg(p) - 1.$$

Wenn q keine Nullstelle hat ...

Achtung: x^2-1

hat in $\mathbb{R}^{2\times 2}$

unendlich viele „Nullstellen" ...

Jedes Polynom $p \in \mathbb{K}[X]$

gibt uns eine Funktion

$$\begin{pmatrix} \mathbb{K} \longrightarrow \mathbb{K} \\ t \longmapsto p(t) \end{pmatrix},$$

genannt Polynomfunktion.

Korollar 3.4.15 $\qquad$ $\mathbb{K}$ Körper

(a) Die Abbildung

punktw. Mult.

$$\Phi : \mathbb{K}[X] \longrightarrow \left(\mathbb{K}^{\mathbb{K}}, +, \bullet, \cdot\right),$$

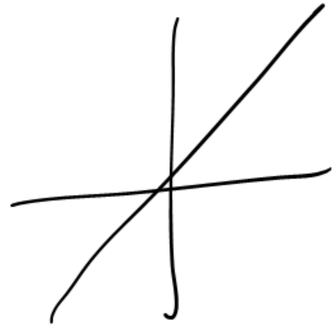
die jedes (abstrakte) Polynom auf die dazugehörige Polynomfunktion abbildet, ist ein $\mathbb{K}$-Algebra-Homomorphismus.

(b) Φ injektiv $\iff$ $\mathbb{K}$ hat ∞ viele Elemente

(c) Φ surjektiv $\iff$ $\mathbb{K}$ hat endlich viele Elemente.

(a) $A = (\mathbb{K}^{\mathbb{K}}, +, \cdot, \cdot)$

$f = \mathrm{id}_{\mathbb{K}} : t \longmapsto t$



5.4.11

$\exists\; \Phi : \begin{pmatrix} \mathbb{K}[X] \longrightarrow \mathbb{K}^{\mathbb{K}} \\ X \longmapsto f \end{pmatrix}$ Alg-Homo.

(b) „$\Longrightarrow$" Φ injektiv.

$\underbrace{\mathbb{K}[X]}_{} \longrightarrow \mathbb{K}^{\mathbb{K}}$

∞ viele Elemente.

$\Longrightarrow \mathbb{K}^{\mathbb{K}}$ ∞ viele El.

$\Longrightarrow \mathbb{K}$ ∞ viele El.

"$\Longleftarrow$": Angenommen $|\mathbb{K}| = \infty$. z.z: Φ inj.

$p \in \ker \Phi$ z.z: $p = 0$

Angenommen, $p \neq 0$.

$\deg(p) = n \in \mathbb{N}_0$

$\Longrightarrow$ p hat höchstens n Nullstellen.

Aber: $\forall t \in \mathbb{K}$ $p(t) = 0$. $\lightning$

(c) „$\Rightarrow$": Wenn Φ surjektiv ist, dann ist jede Funktion von $\mathbb{K}$ nach $\mathbb{K}$ eine Polynomfunktion.

Also auch

$$f: \mathbb{K} \to \mathbb{K}$$
$$x \mapsto \begin{cases} 1 & \text{falls } x = 0 \\ 0 & \text{sonst.} \end{cases}$$

Das dazugehörige Polynom $p \in \mathbb{K}[X]$ ist nicht das Nullpolynom, weil $p(0) = f(0) = 1$.

Also hat p einen Grad $n = \deg(p) \in \mathbb{N}_0$ und höchstens n Nullstellen in $\mathbb{K}$.

Also muss $\mathbb{K}$ endlich sein.

„$\Leftarrow$": Angenommen $\mathbb{K}$ ist endlich $|\mathbb{K}| = m < \infty$.

$\mathbb{K} = \{\lambda_1, \dots, \lambda_m\}$

$\forall k \in \{1, \dots, m\}$ setze

$$p_k = \prod_{j \neq k} (X - \lambda_j) \in \mathbb{K}[X].$$

Dann gilt: $p_k(x) = 0$ falls $x \neq \lambda_k$

Die Funktionen $f_k = \Phi(p_k) \in \mathbb{K}^{\mathbb{K}}$

sind somit linear unabhängig und eine Basis für den m-dim. VR $\mathbb{K}^{\mathbb{K}}$.

Also enthält $\mathrm{Bild}(\Phi)$ eine Basis von $\mathbb{K}^{\mathbb{K}}$.

Also ist Φ surjektiv. $\blacksquare$